

STAT

Sanitized Copy Approved for Release 2011/07/15 : CIA-RDP87T00623R000100020024-9

Page Denied

Sanitized Copy Approved for Release 2011/07/15 : CIA-RDP87T00623R000100020024-9

SAISS

SUBCOMMITTEE ON
AUTOMATED INFORMATION
SYSTEMS SECURITY

EXECUTIVE SECRETARY

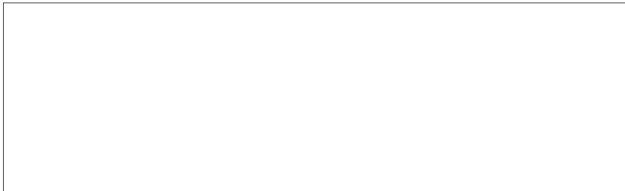
SAISS-042-85
25 July 1985

**MEMORANDUM FOR THE MEMBERS AND OBSERVERS OF THE SUBCOMMITTEE
ON AUTOMATED INFORMATION SYSTEMS SECURITY**

**SUBJECT: Draft Policies on National Automated Information
Systems Security Education and Training and National
Automated Information Systems Security Awareness
Program**

1. Please reference SAISS-036-85 (WG#4-002-85), same subject, dated 10 July 1985.
2. Attached for your review are the final draft policy directives on the subject topics. The SAISS is scheduled to vote on adoption of these directives at its 01 August 1985 meeting.

STAT


Executive Secretary
Subcommittee on Automated
Information Systems Security

Encl:
a/s

FOR OFFICIAL USE ONLY

Page Denied

Next 4 Page(s) In Document Denied

NTISSP NO. 1
DATE: 17 June 1985

NTISS

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

**NATIONAL POLICY
ON
APPLICATION OF COMMUNICATIONS
SECURITY TO U.S. CIVIL AND
COMMERCIAL SPACE SYSTEMS**

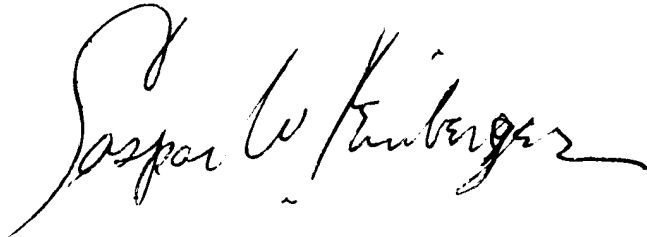
**EXECUTIVE AGENT FOR NATIONAL
TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY**

FOREWORD

The use of satellites for the transmission of U.S. Government and Government contractor telecommunications is expanding rapidly. The "National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems" was developed by the National Telecommunications and Information Systems Security Committee (NTISSC) in recognition of a need to protect U.S. space systems.

It is a policy to protect both the relayed telecommunications transmitted over space system circuits, and the command/control uplink. Government or Government contractor use of civil space systems for telecommunications is limited to those protected by approved techniques. The Government shall encourage the similar protection by approved means of all commercial space systems.

This policy is effective immediately, and supersedes NCSC-10, "National Policy for Protection of U.S. National Security Related Information Transmitted Over Satellite Systems," dated 26 April 1982.

A handwritten signature in dark ink, appearing to read "Jasper W. Funderburg". The signature is fluid and cursive, with a long horizontal stroke at the end.

NATIONAL POLICY
ON
APPLICATION OF COMMUNICATIONS SECURITY TO U.S.
CIVIL AND COMMERCIAL SPACE SYSTEMS

SECTION I - POLICY

1. Government classified and Government or Government contractor national security related information transmitted over satellite circuits shall be protected by approved techniques from exploitation by unauthorized intercept.

2. Government or Government contractor use of U.S. civil (Government-owned but non-DoD) and commercial satellites launched five years from the date of this policy shall be limited to space systems using accepted techniques necessary to protect the command/control uplink. Nothing in this policy shall preclude use of satellites that do not employ command/control uplink protection if those satellites are launched prior to or during the specified five-year period.

3. The need for and means to protect the command/control uplink associated with civil satellite systems, intended exclusively for unclassified missions, will be determined by the organization responsible for the satellite system in coordination with the National Security Agency.

SECTION II - EXCEPTIONS

4. Exceptions to this policy may be granted by the NTISSC in consultation with Federal departments and agencies, as well as the private sector.

SECTION III - DEFINITIONS

5. Space systems consist of the spacecraft or satellite, command ground station, data acquisition stations, telecommunications, and command/control uplink.

SECTION IV - HEADS OF DEPARTMENTS

6. The Director, National Security Agency, in coordination with other departments or agencies as appropriate, shall assess space systems telecommunications, and command/control uplink functions to determine their vulnerability to unauthorized use and provide approved protection techniques and guidance.

7. Nothing in this policy shall relieve the heads of Federal departments and agencies of their authority and responsibility for executing other measures to assure the adequate protection of their telecommunications.